

## Cisco Security Agent and Microsoft DNS 0Day Exploit

PB405353

### Summary

A vulnerability has been discovered in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 and 2003 operating systems. The Microsoft DNS service Remote Procedure Call (RPC) implementation contains a stack buffer overflow. This vulnerability may allow a remote attacker to execute arbitrary code with SYSTEM privileges.

This vulnerability has already been exploited in several attacks. Cisco® has obtained exploit files, and has confirmed that the Cisco Security Agent is effective in stopping these exploits, using the default security policy configuration. Current supported versions of Cisco Security Agent 4.5.x, 5.0.x, 5.1.x, and 5.2.x are all effective in stopping the exploits seen to date.

### Details of the Vulnerability

Details of the vulnerability are documented by Microsoft<sup>1</sup> and by the Computer Emergency Response Team (CERT)<sup>2</sup>:

A stack-based buffer overflow vulnerability in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 and 2003 operating systems allows remote attackers to execute arbitrary code, by sending a specially crafted RPC packet to the RPC management interface of an affected system.

RPC is a protocol that a program can use to request a service from a program located on another computer in a network. RPC helps with interoperability because the program using RPC does not have to understand the network protocols that are supporting communication. In RPC, the requesting program is the client and the service-providing program is the server.

### How Cisco Security Agent Stops the Exploit

Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- The receipt of a TCP connection from a remote IP address
- Execution of a system function from a buffer, through a buffer overflow
- The attacked service attempted to execute a command shell (CMD.EXE)

<sup>1</sup> Microsoft: <http://www.microsoft.com/technet/security/advisory/935964.msp>

<sup>2</sup> CERT Advisory: <http://www.kb.cert.org/vuls/id/555920>

This testing is shown in Figure 1.

**Figure 1.** Cisco Security Agent Default Configuration Stops the MS DNS 0-Day Exploit (Tested on Cisco Security Agent 5.2)

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface. The 'Events' section is active, displaying an event log with three events. The events are as follows:

#	Date	Host	Severity	Event
3	4/17/2007 10:43:49 PM	w2ksrvsp4	Alert	TESTMODE: The current application 'C:\WINNT\System32\dns.exe' (as user NT AUTHORITY\SYSTEM) attempted to execute the new application 'C:\WINNT\System32\cmd.exe'. The operation would have been denied. <a href="#">Details</a>   <a href="#">Rule 461</a>   <a href="#">Wizard</a>   <a href="#">Find Similar</a>
2	4/17/2007 10:43:49 PM	w2ksrvsp4	Notice	TESTMODE: The process 'C:\WINNT\System32\dns.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\System32\dns.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' <a href="#">Details</a>   <a href="#">Rule 186</a>   <a href="#">Wizard</a>   <a href="#">Find Similar</a>
1	4/17/2007 10:43:46 PM	w2ksrvsp4	Alert	TESTMODE: The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 139 from 192.168.58.134 using interface Wired\AMD PCNET Family PCI Ethernet Adapter. The operation would have been denied. <a href="#">Details</a>   <a href="#">Rule 59</a>   <a href="#">Wizard</a>   <a href="#">Find Similar</a>

**Note:** The exploit was tested at Cisco, with the agent in Test mode, which will cause the agent to alert (but not block) malicious behavior. This was done to observe all possible ways that the Cisco Security Agent default policies would stop the exploit. When the agent is in Protect mode (the typical operational configuration), the first rule would kill the exploit: no subsequent events would be seen, since the exploit would be terminated before it could perform any malicious actions.

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of "day-zero" protection. This is similar to what Cisco has seen with earlier exploits and worms—the default Cisco Security Agent configuration stopped the exploit, with no binary or policy updates required. The following is a partial list of prior worms and exploits that Cisco Security Agent has stopped via the default security policy settings:

Exploits	Worms	Exploits	Worms
ANI 0Day	OS vulnerability	MS06-035	OS vulnerability
Bagle	E-mail worm	MS06-040	OS vulnerability
BigYellow	Network worm	MS06-070	OS vulnerability
Blackworm	Network worm	MS07-014	Application vulnerabilities
Blaster	Network worm	Excel hlink dll	Application vulnerability
Bugbear	E-mail worm	MS RDS ActiveX	OS vulnerability
Code Red	Network worm	MS XML Core Svs	OS vulnerability

Exploits	Worms	Exploits	Worms
Debplot	Network worm	Nimda	Network worm
Fizzer	E-mail worm	Pentagone/Gonner	E-mail worm
Gator/Gain	Spyware	Sasser	Network worm
Hotbar	Spyware	Sircam	E-mail worm
HTTP Dir Traversal	Web server vulnerability	Sobig	E-mail worm
IE Text Range	Application vulnerability	Storm Trojan	E-mail worm
IE VML BO	Application vulnerability	WMF Oday	OS vulnerability
SQL Slammer	Network worm	Word BO	Application vulnerability
SQL Snake	Network worm	W32.Rinbot.H	Network worm
JPEG/GDI+	Malware downloader	Zotob	Network worm
MyDoom	E-mail worm		

This exploit is only the latest example of new and mutating attacks that can seriously affect an organization's computing and network environments. The key to stopping these new attacks is two-fold: the ability to stop the attack without requiring any changes to the default configuration, and multiple rules in the default policies that provide defense in depth.



Americas Headquarters  
Cisco Systems, Inc.  
170 West Taftman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 453-3418 (toll free)  
Fax: 408 527-0689

Asia Pacific Headquarters  
Cisco Systems, Inc.  
155 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Europe Headquarters  
Cisco Systems International BV  
Hertfordpark  
Hertfordparkweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www.europe.cisco.com  
Tel: +31 20 600 020 0/91  
Fax: +31 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access, Register, Attend, EPX, Catalyst, CSDA, CCIP, CCIE, CCIP/CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Discovery/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IQS, iPhone, IPTV, IQ Director, the IQ logo, IQ Net, Roadshow, Scorecard, iQuickStart, iStream, iLinksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RaptorLIX, ScriptShare, SideCast, SMARTnet, StackWise, The Router, Way to Increase Your Internet Quotient, and Thousand are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (07012)